Information Security

Rob McKinney

Wireless Network Policy - Draft

- Deploy adequately secure wireless networks.
- Deployment planning shall consider the risks associated with implementing wireless technologies, particularly as they affect sensitive information.
- Wireless network deployments shall:
  - Follow NIST developed FIPS and guidelines, and HHS and IHS directives. Where conflicts in these documents arise questions shall be directed to the IHS CIO for resolution.
  - Comply with HIPAA and FISMA requirements.

Wireless Network Policy - Draft

- Risk Assessment
- Site survey
- Deploy registered and approved wireless access points
- Deploy access points in standard configuration properly secured
- Client devices configured with standard protections
- Ensure proper client access and mutual authentication
- Separate the WLAN from the wired
- IHS ISSO shall establish standards

Adequate Security

- Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls.

Requirements

- Adequate security
  - Sensitive information – communication channels that provide mutual authentication, integrity, and confidentiality
    - Cryptographic mechanisms – shall comply with FIPS
  - Non-sensitive information – communication channels

Possible Wireless Network Solutions

- ***Fortress Technologies*** **solutions are recommended for new and existing WLAN implementations.**

- ***A VPN*** **solution using Windows XP or 2000 SP3 clients and a FIPS 140 compliant, VPN capable router or firewall with strong authentication such as digital certificates or RADIUS is only recommended for limited scale implementations.**

Possible Wireless Network Solutions

- ***A VPN*** **solution using IBM's ICC cryptographic module for Linux devices with strong authentication such as certificate or RADIUS solutions is recommended.**
- **The *3eTI* products are not recommended unless there is a specific need for deployment in harsh conditions where limited network capacities are sufficient.**
- **The ReefEdge products are not recommended at this time. They offer FIPS 140 level 2 compliant solutions that work with any AP and conform to Wi-Fi Protected Access standards. However, only their edge controller has been certified compliant and only with 3DES for encryption.**

Indian Health Service Information Security Plan and Strategy FY2004 - FY2009

In Support of IHS Goals and Initiatives

- Providing a secure and trusted IT environment
- Enhancing the ability of the Nation's healthcare system to effectively respond to bioterrorism and other public health challenges
- Achieving excellence in IT management practices

Mission Statement

- ***Provide an agency-wide secure and trusted information technology environment in support of IHS' commitment, in partnership with American Indian and Alaska Native people, to raising their physical, mental, social, and spiritual health to the highest level.***

Vision

- ***Develop and institutionalize an information security program that:***
  - ***Promotes agency-wide security awareness and compliance***
  - ***Facilitates collaboration and encourages partnership among Agency entities in development and support of information security requirements***
  - ***Helps security personnel understand and implement information security policies and procedures***
  - ***Encourages performance measurement and improvement***

Goals

- *1 – Improve the overall information security posture to adequately assure the confidentiality, integrity, and availability of information and information resources*
- *2 – Create an environment where all employees' actions reflect the importance of information security*
- *3 – Establish and maintain consistent agency-wide policies and procedures to protect IHS' information and information systems from abuse and inappropriate use*
- *4 – Ensure minimum security standards agency wide, consistent with Federal guidelines and best practices*
- *5 – Support integration of information security into IHS lines of business*
- *6 – Establish program metrics to measure information security program performance*

Goals & Objectives

- ***Goal 1 – Improve the overall information security posture to adequately assure the [illegible] information resources***

1.8 – Implement agency-wide use of Federal [illegible] (PKI)

[illegible] Information Security Management Act (FISMA) Plan of Action and Milestones (POA&M) Process and tool

[illegible] Accreditation (C&A) for every major application (MA) and general support system (GSS)

Objectives

- *Goal 1 – Improve the overall information security posture to adequately assure the confidentiality, integrity, and availability of information and information resources*
  - *1.1 – Implement Public Key Infrastructure (PKI)*
  - *1.2 – Implement Certification and Accreditation (C&A) Process*
  - *1.3 – Implement Plan of Action and Milestones (POA&M) Process*
  - *1.4 – Implement Configuration Management (CM) and general support system (GSS)*

Goals & Objectives

- ***Goal 2 – Create an environment where all employees' actions reflect the importance of information security***

2.1 – Provide role-based training ***2.2 – Provide awareness training***

Objectives

- *Goal 2 – Create an environment where all employees' actions reflect the importance of information security*

2.1 – All users receive information security awareness training

2.2 – Provide role-based training

Goals & Objectives

- ***Goal 3 – Establish and maintain consistent agency-wide policies and procedures to protect IHS' information and information systems from abuse and inappropriate use***

3.1 – Develop, disseminate and maintain agency policies and procedures that comply with applicable federal requirements

3.2 – Provide appropriate training to all IHS staff and contractors on agency policies and procedures

Objectives

- *Goal 3 – Establish and maintain consistent agency-wide policies and procedures to protect IHS' information and information systems from abuse and inappropriate use*
  - *3.2 – Develop and implement an information security program that is consistent with agency-wide policies and procedures and all applicable federal requirements and disseminate*

Goals & Objectives

- *Goal 4 – Ensure minimum security standards agency wide, consistent with Federal guidelines and best practices*
  - *4.1 – Establish a capability to develop, document, validate, and disseminate standard hardware and software configurations*
  - *4.2 – Establish a capability and coordination with IHS personnel in development and maintenance of standard hardware and software components and configurations consistent with NIST and other federal guidelines*

Objectives

- ***Goal 4 – Ensure minimum security standards agency wide, consistent with Federal guidelines and best practices***

4.1 – Establish a capability to develop, document, and implement standard hardware and software components and configurations

4.2 – [illegible] IHS [illegible] in accordance with NIST and other federal guidelines

Goals & Objectives

- *Goal 5 – Support integration of information security into IHS lines of business*

5.1 – Accurately identify information security funding requirements to ensure that budget requests are responsive to information security priorities

5.2 – Ensure IT investment has a documented plan for addressing security at each stage in the investment lifecycle, including incorporation of security into current IT capital plans

Objectives

- *Goal 5 – Support integration of information security into IHS lines of business*

5.1 – Annually identify information security funding requirements at each stage of the investment lifecycle, including incorporation of security into current IT capital plans

5.2 – Ensure that IT investments have documented plan for addressing security at each stage budget requests are responsive to information security priorities

Goals & Objectives

- ***Goal 6 – Establish program metrics to measure information security program performance***

6.1 – Develop, apply, and maintain plans to establish metrics

6.2 – Develop, apply, and maintain plans to report progress results

Objectives

- *Goal 6 – Establish program metrics to measure information security program performance*

6.1 – [illegible]
6.2 – [illegible]
6.3 – [illegible] to progress results

Objectives

- *1.1 – Complete and maintain National Institute of Standards and Technology (NIST) Certification and Accreditation (C&A) for every major application (MA) and general support system (GSS)*
- *1.2 – Achieve and maintain Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance*
- *1.3 – Complete and maintain Privacy Impact Assessments (PIAs) for every MA and GSS*
- *1.4 – Ensure information systems are adequately protected*
- *1.5 – Implement HHS' Public-Key Infrastructure (PKI) initiative across IHS*
- *1.6 – Complete and maintain E-Authentication requirements*
- *1.7 – Develop an IHS Incident Response capability*
- *1.8 – Implement agency wide use of Federal Information Security Management Act (FISMA) Plan of Action and Milestones (POA&M) Process and tool*
- *1.9 – Implement an automated patch management system agency wide*

Objectives

- *2.1 – All users receive information security awareness training*
- *2.2 – Provide role-based training*

Objectives

- ***3.1 – Update information security policies to comply with NIST standards and all applicable federal requirements***
- ***3.2 – Develop agency-wide information security procedures to comply with NIST standards and all applicable federal requirements and disseminate***
- ***3.3 – Promote implementation of agency-wide policies and procedures at all levels of IHS***
- ***3.4 – Promote cooperation and coordination with Area personnel in development and maintenance of agency-wide policies and procedures***

Objectives

- ***4.1 – Establish a capability to develop, document, validate, and disseminate standard hardware and software components and configurations in accordance with NIST and other federal guidelines***
- ***4.2 – Promote cooperation and coordination with IHS personnel in development and maintenance of standard hardware and software components and configurations***

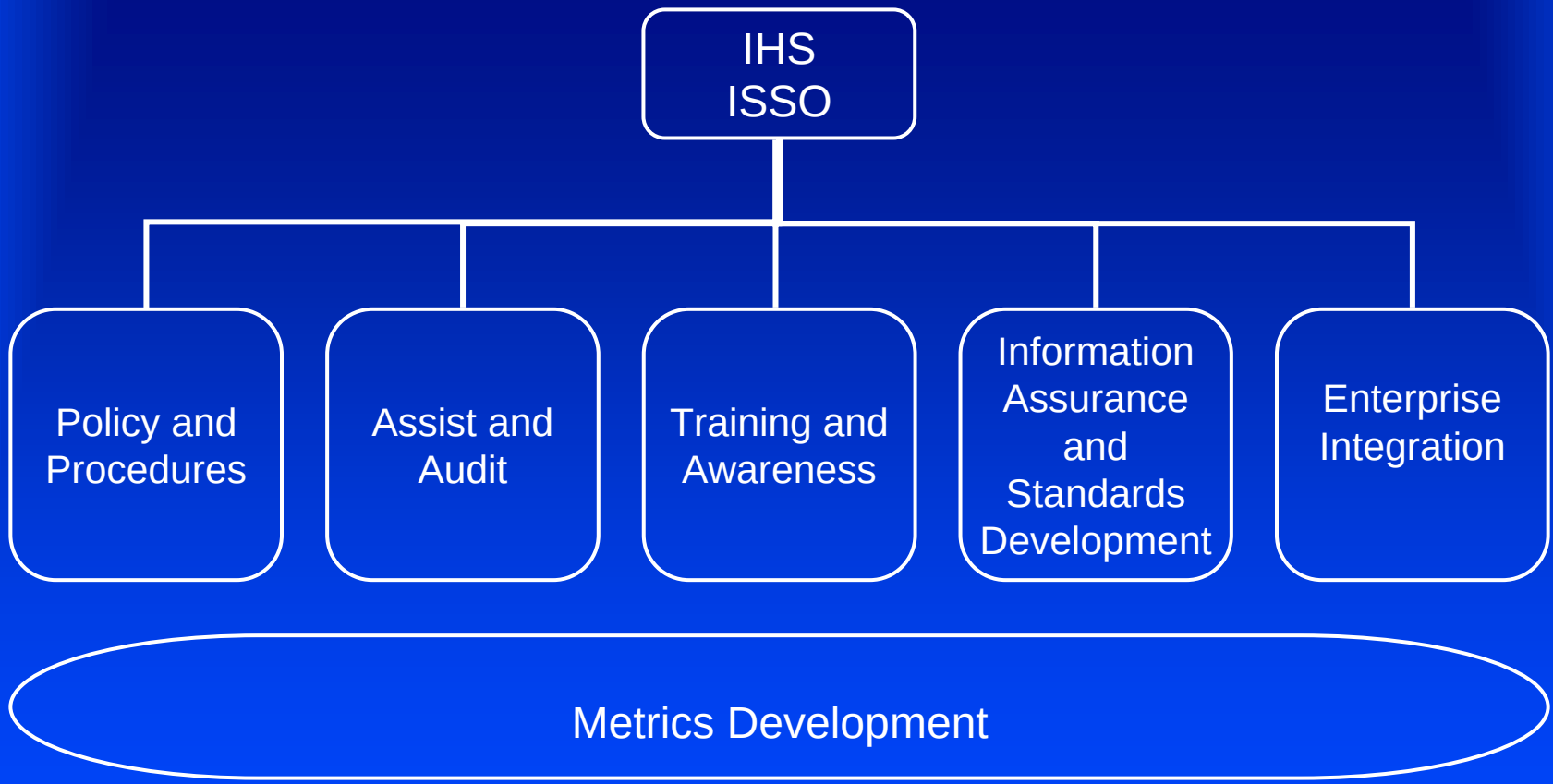
Objectives

- ***5.1 – Ensure IT investment has a documented plan for addressing security at each stage in the investment lifecycle, including incorporation of security into current IT capital plans***
- ***5.2 – Accurately identify information security funding requirements to ensure that budget requests are responsive to information security priorities***

Objectives

- *6.1 – Define measurable program results and establish metrics*
- *6.2 – Periodically apply metrics to determine progress*
- *6.3 – Develop or modify, and implement action plans according to progress results*

Functional Areas



Functional Area Descriptions

Policy and Procedures	**Draft, coordinate, and disseminate policies and procedures in support of the IHS Information Security Program**
Assist and Audit	**Assist IHS facilities' information security efforts and Audit IHS facilities for compliance with information security program and system plans, policies, procedures, and standards**
Training and Awareness	**Provide data collection and instructional services, produce and implement information security and IT training and awareness products**
Information Assurance and Standards Development	**Track and provide information security advisories and recommendations, track and maintain system inventories, track and disseminate information security requirements, develop and issue software and hardware information security related configuration standards**
Enterprise Integration	**Provide support and facilitate integration of information security into enterprise initiatives**

Policies and Procedures

- Conduct policy and procedure assessment activities
  - Policy identification and baseline, including IHS policies and handbook review and Area policies and procedures review
  - Conduct policy GAP analysis
  - Review policy infrastructure
  - Analyze internal interdependencies
  - Analyze external interdependencies
  - Develop Policies and Procedures performance measures
- Conduct policy and procedures performance activities
  - Develop Policies and Procedures document management
  - Revise handbooks
  - Revise policies
  - Revise procedures

Assist and Audit

- Provide on the spot (ad hoc) role-based information security training
- Assist in remediation of identified unacceptable risks
- Provide incident response capabilities and support
- Review program and system level information security for compliance and effectiveness
- Provide IHS ISSO office an avenue to interact with and promote coordination and cooperation with Area Facility personnel for P&P and standards efforts

Training and Awareness

- Collect data on information security training and awareness
- Develop and maintain an annual information security awareness course
- Develop and maintain a role-based information security training program
- Develop and maintain an information security training module in New Hire Orientation
- Provide periodic and ad hoc security awareness training and information security related news

Information Assurance and Standards Development

- Monitor antivirus and vulnerability notification sites
- Disseminate pertinent antivirus and vulnerability alerts
- Investigate mitigating recommendations for compatibility with IHS systems
- Verify recommended patches for compatibility with IHS systems and disseminate
- Maintain system inventories
- Track requirements compliancy such as C&A, PIA, risk assessments, and security plans
- Coordinate with and disseminate information from IDS services
- Develop, disseminate, and test compatibility with IHS systems, standard hardware and software configurations
- Evaluate C&A, FISMA POA&M, and IHS information security indicators and incorporate with operational and user needs to assess IHS information security posture, trends and requirements
- Investigate solutions for emerging information security requirements

Enterprise Integration

- Many of the activities for this function are determined by progress made at the IHS enterprise level with each of the areas listed below:
  - Strategic Planning
  - Enterprise Architecture
  - Capital Planning and Investment Control Program
  - Continuity of Operations Plan and Program
  - Managed Security Services Initiative
  - Other Enterprise Initiatives

Metrics Development

- Define measurable and meaningful metrics
- Apply, track, collect, and report metrics
- Evaluate metrics and trends to make system and program improvement recommendations

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2004		
Assist and Audit 1 Contractor	Initiate A&A capability Initiate plans for dedicated Area Office ISSOs & ID funding	+ $150K
FY2005		
Assist and Audit 1 Position Information Assurance & Standards Development 1 Position	Add to A&A capability and initiate IA&SD capability Initiate plans for dedicated Area Office ISSOs & ID funding	+ $309K

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2006		
Assist and Audit 2 Positions	Add to A&A, define two A&A teams	+ $2.07M
Information Assurance & Standards Development 1 Position	Initiate IHS Incident Response capability	
Information Security Support at Area Offices 10 Positions	Add to IA&SD capability Dedicated Area Office ISSOs at all Area Offices & ID funding	

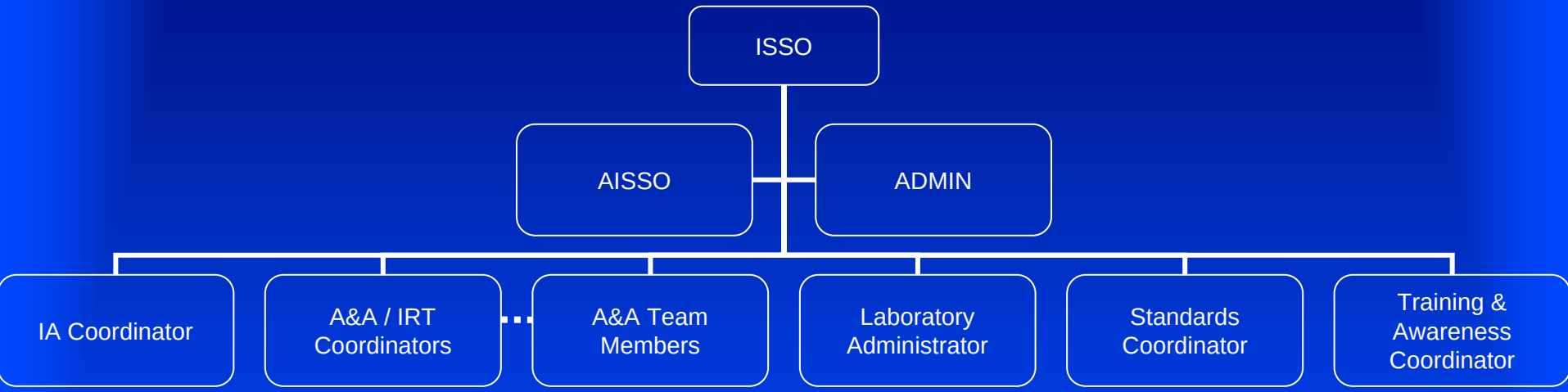
Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2007		
Assist and Audit 2 Positions	Add to A&A and IR capability	+ $492K
Training & Awareness 1 Position	Enhance T&A capability and initiate role-base training program & ID funding	
FY2008		
Assist and Audit 2 Positions	Complete two A&A and IR teams & ID funding	+ $338K

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2009		
	Evaluate capabilities and requirements – plan adjustments as necessary & ID funding	

Organization



Basic Duties and Responsibilities

- Information Assurance Coordinator – information security alerts / notifications, antivirus software, patch management, software configuration checks, web cookies, penetration and vulnerability testing, and IDS
- Assist and Audit / Incident Response Team Coordinator – IRT, Assist and Audit Team Coordinator, and lessons learned
- Assist and Audit Team Member – training and education, audit, remediation, network information maintenance
- Standards Coordinator – system configurations, hardware and software certification and accreditation, privacy impact, risk, and e-authentication assessments

Basic Duties and Responsibilities

- Laboratory Administrator – system administrator, IA, Assist and Audit Team support, and general support
- Training and Awareness Coordinator – training program definition, implementation, maintenance, and coordination, and awareness program maintenance
- Assistant – policies, procedures, and guidance maintenance, program metrics, requirements (i.e., Department, legislative, Administration) tracking, HIPAA, FISMA, COOP coordination, and program management / project officer functions
- Administrative Assistant – general administration

Staffing Source Options

- *Alternative A*
  - All federal employees (14)
- *Alternative B*
  - All federal employees (7) except; Assist Team members and Laboratory position, which would be contracted (7)
- *Alternative C*
  - All contractors (9) except; Assistant, Admin, Assist and Audit / Incident Response Team Coordinators, and Standards, which would be federal employees (5)
- *Alternative D*
  - All contractors (12) except; Assistant and Admin, which would be federal employees (2)

Information Security Support Team Composition

- Information Assurance Coordinator (1 – GS 12/13)
- Assist and Audit / Incident Response Team Coordinator (2 – GS 13)
- Assist and Audit Team Member (6 – GS 11/12)
- Standards Coordinator (1 – GS 12/13)
- Laboratory Administrator (1 – GS 11/12)
- Training and Awareness Coordinator (1 – GS 11)
- Assistant (1 – GS 13)
- Administration Support (1 – GS 5)

HIPAA Security

HIPAA Security

- Risk Assessment – Initial Step
- Follow-up Steps

Risk Assessment – Initial Step

- GSA Contract Vehicle
  - SOW written to conduct risk assessment IAW NIST Guidelines and to cover HIPAA, C&A, and e-authentication
  - Tribal facilities can use the contract vehicle
  - Navajo moving forward with 7 facilities
  - Plan from each Area
  - Funds up front

Risk Assessment – Initial Step

- *Nominal Entity Descriptions*
  - Level 1 – 2-25 users, simple LAN with associated hubs, perhaps one or two routers or switches, possibly a firewall - $10K
  - Level 2 – 25 – 200 users, one to three buildings with separate LAN's and associated hubs, routers, and or switches, possibly a firewall and servers - $18K
  - Level 3 – 200 – 400 users, one to five buildings with separate LAN's possibly a mall WAN and associated hubs, routers, and switches, one or two firewalls, various servers - $26K
  - Level 4 – 400 - 700 users, one to five buildings with separate LAN's possibly a small WAN and associated hubs, routers, and switches, one or more firewalls, various servers - $43K

Follow-up Steps

- Enter weaknesses into ISDM (FISMA POA&M) tool
- Conduct Risk Management
  - NIST SP 800-30
  - FIPS 199 Categorization
    - RPMS – High
    - GSS w/RPMS – High
  - Implement, and test and evaluate controls
    - NIST SP 800-53 - Draft
    - FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*,

ISDM and PIA Nomenclature Proposal

- Use the 300 identifiers we now have modified in a similar fashion to the following.
- IHSNet encompassing all GSS's:
  - IHSNet Project ID = 09-17-02-01-01-1010-02
  - IHSNet Project ID modified = 09-17-02-01-01-1010-02-[Area or Misc. #]-[facility #]

ISDM and PIA Nomenclature Proposal

Area or Misc. #	facility #
Aberdeen – 1	Area Office – 1
	Belcourt - 2
Alaska – 2	.
.	.
.	.
Tucson – 12	
Misc – 13	HQE – 1
	HQW – 2

Aberdeen Area Office

- GSS Project ID = *09-17-02-01-01-1010-02-*1-1

ISDM and PIA Nomenclature Proposal

- For RPMS we need something similar
- RPMS Project ID modified = 009-17-04-01-01-1010-02-[Additional project #]

Additional Project #

EHR – 1

EDR – 2

Mobile Mammography – 3

PHN project – 4

Etc.

EHR Project ID = *009-17-04-01-01-1010-02-1*

Follow-up Steps

- Conduct IHS-wide policies and procedures Gap Analysis
- Conduct entity-level policy, procedures, and practices Gap Analysis
- Implement policies and procedures
- Complete Security Awareness Training
  - Fiscal year cycle – 100% by 1 Sep

Follow-up Steps

- Business Partner Agreements
  - For all entities connecting to IHS systems and interacting with IHS information
- Complete Privacy Impact Assessments (PIA)

Follow-up Steps

- NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
  - **http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf**

HHS Security Mandates

Current HHS Topics

- FISMA
  - ISDM
  - SSAT
  - PIA
  - C&A
  - Security training awareness
  - Correlating 300/53's, C&A's/e-authentication, PIA's Inventories
- HIPAA
  - BPA

IHS Security Priorities

Defense in Depth

- Resources
- HIPAA – BPA's (Compacts / contracts)
- FISMA – BPA's (Compacts / contracts)
- Implementing policies and procedures
- Automated patching
- Standard configurations
- Remote access
- Role-based training

Certification & Accreditation

- 5 to 6 months for 3 people expending approximately 3,000 total person hours
- Automated document control systems
  - SecureInfo Corporation
    - Risk Management System (RMS)
    - Pilot
    - C&A Training

SecureInfo RMS

Quantity	5	100	200	400
License Fee/User	$4,309	$3,591	$2,334	$2,334
Total License Fees	$21,546	$373,464	$606,879	$1,073,709
Maintenance	$5,387	$93,366	$151,720	$268,427
Installation	$4,972	$4,972	$4,972	$4,972
RMS 2 Day Workshop	$9,562	$66,934	$133,868	$258,174
Total First Year Cost	$41,467	$538,736	$897,439	$1,605,282

C&A Training

- Practical ST&E Workshop
  - Individual - $1,912
  - Class of 20 - $19,125
- C&A Process
  - Individual - $992
  - Class of 20 - $9,925
- C&A Process Advanced Concepts
  - Individual - $1,912
  - Class of 20 - $19,125
- Designated Approval Authority (DAA)
  - Class of 25 - $1,496

Risk Assessment – NIST 800-30

- Step 1 System Characterization
- Step 2 Threat Identification
- Step 3 Vulnerability Identification
  - Track 4: Hacker Techniques, Exploits and Incident Handling – 6 days - $2,900
  - Track 7: Auditing Networks, Perimeters and Systems - 6 Days - $2,900
- Step 4 Control Analysis
  - Track 2: Firewalls, Perimeter Protection and VPNs - 6 days - $2,900
  - Track 5: Securing Windows - 6 Days - $2,900
  - Track 6: Securing Unix/Linux - 6 Days - $2,900
- Step 5 Likelihood Determination
- Step 6 Impact Analysis
- Step 7 Risk Determination
  - Track 9: Intro to Information Security – 6 days **- $2,900**
- Step 8 Control Recommendations
- Step 9 Results Documentation